SHARP LOWER BOUNDS FOR THE ASYMPTOTIC ENTROPY OF SYMMETRIC RANDOM WALKS

SÉBASTIEN GOUËZEL, FRÉDÉRIC MATHÉUS, FRANÇOIS MAUCOURANT

Abstract. The entropy, the spectral radius and the drift are important numerical quantities associated to any random walk with finite second moment on a countable group. We prove an optimal inequality relating those quantities, improving upon previous results of Avez, Varopoulos, Carne, Ledrappier. We also deduce inequalities between these quantities and the volume growth of the group. Finally, we show that the equality case in our inequality is rather rigid.

1. Introduction and main results

Let Γ be a finitely generated group and μ a probability measure on Γ. The right random walk associated with the pair (Γ, μ) is the Markov chain on Γ whose transition probabilities are defined by $p(x, y) = \mu(x^{-1}y)$. A realization of the random walk starting from the identity is given by $X_0 = e$ and $X_n = \gamma_1 \cdots \gamma_n$ where $(\gamma_i)_i$ is an independent sequence of Γ-valued μ-distributed random variables. The law of X_n is the n-fold convolution μ^{*n} of μ.

Several numerical quantities were introduced to describe the asymptotic behavior of X_n. The asymptotic entropy h, the spectral radius ρ and the drift ℓ of the random walk with respect to a given finite set S of generators are defined by

$$h = \lim_n -\frac{1}{n} \sum_g \mu^{*n}(g) \log \mu^{*n}(g),$$

$$\rho = \limsup_n \sqrt[n]{\mu^{*n}(e)} \leqslant 1,$$

$$\text{and} \quad \ell = \lim_n \frac{1}{n} \sum_g |g| \, \mu^{*n}(g),$$

where $|\cdot|$ is the word length with respect to S.

Denote by F and G the functions defined, for $x \in [0, 1)$, by

$$F(x) = x \log\left(\frac{1+x}{1-x}\right) \quad \text{and} \quad G(x) = 1 - \sqrt{1 - x^2}. \tag{1.1}$$

In this paper, we prove the following:

Date: October 18, 2012.

2010 *Mathematics Subject Classification.* 05C81, 60B15, 60J50.

Key words and phrases. Random walk, countable group, entropy, spectral radius, drift, volume growth, Poisson boundary.

Theorem 1.1. *Let Γ be a finitely generated group and μ a symmetric probability measure on Γ such that $M_2(\mu) := \left(\sum_g |g|^2 \mu(g)\right)^{1/2}$ is finite. Let $A, B : [0,1) \to \mathbb{R}$ be two nondecreasing functions such that*

$$A + B \circ G \leqslant F.$$

Then one has

$$A\left(\frac{\ell}{M_2(\mu)}\right) + B(1-\rho) \leqslant h.$$

If $A = 0$ in the above statement, then $B(1-\rho) \leqslant h$ holds for any nondecreasing function B such that $B \circ G \leqslant F$ and for any symmetric probability measure μ *without any moment condition*.

Remark 1.2. If the second order moment $M_2(\mu)$ is finite, then so is $M_1(\mu) := \sum_g |g| \mu(g)$, hence $\ell < +\infty$. Moreover, if μ is symmetric, then $\ell < M_1(\mu) \leqslant M_2(\mu)$.

The entropy of a probability measure μ on Γ is $H(\mu) = -\sum_{g\in\Gamma} \mu(g) \log \mu(g)$. If the entropy $H(\mu)$ is finite, then the asymptotic entropy h is also finite. Y. Derriennic proved that $M_1(\mu) < +\infty$ implies $H(\mu) < +\infty$ (see [Der86, Kai98]).

Remark 1.3. The conclusion of Theorem 1.1 does not hold any more if the measure μ is not symmetric. For instance, for the random walk on $\mathbb{Z}$ given by $\mu = p\delta_{-1} + (1-p)\delta_{+1}$, one has $h = 0$ while $\ell = |2p-1|$ and $\rho = 2\sqrt{p(1-p)}$. When $p \neq 1/2$, one gets $\ell > 0$ and $\rho < 1$, hence Theorem 1.1 does not hold in this case.

Remark 1.4. Equality can occur in Theorem 1.1. More precisely, assume that A and B satisfy $A + B \circ G = F$. Let $\Gamma = \mathbb{F}(a_1, \ldots, a_d)$ be the free non-abelian group of rank d over $\{a_1, \ldots, a_d\}$ and μ the uniform measure on $S = \{a_1, \ldots, a_d\}^{\pm 1}$. Then equality holds in this case. Actually, one has $\rho = \frac{\sqrt{2d-1}}{d}$ and $\ell = 1 - 1/d$, hence $G(\ell) = 1 - \rho$. Therefore,

$$A(\ell) + B(1-\rho) = A(\ell) + B \circ G(\ell) = F(\ell) = (1 - 1/d)\log(2d-1) = h.$$

Below, we will further discuss four examples of functions A and B satisfying $A + B \circ G = F$, namely:

- the two "extremal" cases $[A = F,\ B = 0]$ and $[A = 0,\ B = F \circ G^{-1}]$, see Theorems 2.1 and 2.2;
- two intermediate cases $[A(x) = (1+x)\log(1+x) + (1-x)\log(1-x),\ B(x) = -2\log(1-x)]$ and $[A(x) = F(x) - 4G(x),\ B(x) = 4x]$, see Corollaries 2.3 and 2.4.

The first lower bound for the asymptotic entropy is due to A. Avez [Ave76]. He proved that if μ is symmetric and has finite entropy, then $h \geqslant -2\log\rho$. Particularly, the vanishing of h implies $\rho = 1$. The three-line proof of Avez deserves being recalled here: using Jensen's inequality and the symmetry of μ, one has

$$\begin{aligned} -H(\mu^{*n}) &= \sum_{g\in\Gamma} \mu^{*n}(g) \log \mu^{*n}(g) \leqslant \log\left[\sum_{g\in\Gamma} \mu^{*n}(g)\mu^{*n}(g)\right] \\ &= \log\left[\sum_{g\in\Gamma} \mu^{*n}(g)\mu^{*n}(g^{-1})\right] = \log \mu^{*2n}(e). \end{aligned}$$

Therefore

$$\frac{1}{n}H(\mu^{*n}) \geqslant -2\log \sqrt[2n]{\mu^{*2n}(e)},$$

and letting $n \to +\infty$ yields $h \geqslant -2\log\rho$.

Another lower bound relating entropy and the spectral radius has been proved by Ledrappier [Led92]: if μ is symmetric and has finite entropy, then $h \geqslant 4(1-\rho)$. This inequality is better than Avez's for values of ρ close to 1, but it is worse for ρ close to 0.

Lower bounds for the asymptotic entropy h involving the drift ℓ were also considered. Assume that μ is a finitely supported symmetric measure on a group Γ. The right random walk on Γ associated with μ is a special case of finite range reversible Markov chains, for which N. Varopoulos proved the following "basic estimate":

$$\forall g \in \Gamma, \mu^{*n}(g) \leqslant Cn^{3/4}\exp\left[-\frac{|g|^2}{Cn}\right]$$

for some constant C depending only on μ [Var85]. Using Cauchy-Schwarz inequality, he deduced that $h \geqslant \ell^2/C$. Hence, for any finitely supported symmetric measure, one has $h = 0 \implies \ell = 0$.

In the same issue of the *Bulletin des sciences mathématiques*, K. Carne both improved the statement and simplified the proof of Varopoulos' estimate [Car85]. He obtained:

$$\forall g \in \Gamma, \mu^{*n}(g) \leqslant 2\exp\left[-\frac{|g|^2}{2nk^2}\right]$$

where k is the radius of the smallest ball containing the support of μ. The consequence for h and ℓ becomes $h \geqslant \ell^2/2k^2$.

Actually, Carne's estimate can be improved. A careful inspection of his proof enabled J. Lœuillot to prove the following: if μ is a finitely supported symmetric probability measure on a group Γ and k is such that $\mathrm{supp}(\mu) \subset B(e,k)$, then

$$\forall g \in \Gamma, \mu^{*n}(g) \leqslant 2\rho^n\exp\left[-\frac{n}{2}A\left(\frac{|g|}{nk}\right)\right]$$

where A is defined, for $x \in [0,1)$, by $A(x) = (1+x)\log(1+x) + (1-x)\log(1-x)$. (See the Appendix for a proof. Observe that this is the function A involved in Corollary 2.3.) Using Jensen inequality and the convexity of A, he deduced that $h \geqslant A(\ell/k)/2 - \log\rho$ [Lœu11]. This is the first estimate involving both ℓ and ρ.

All these lower bounds for the entropy h involving ℓ rely on estimates of $\mu^{*n}(g)$ and require the measure μ to be finitely supported (and symmetric). Recently, A. Erschler and A. Karlsson proved that $h \geqslant \ell^2/C$ still holds for symmetric probability measures with finite second moment [EK12].

Theorem 1.1 improves all the results mentioned above. Actually, each of these estimates can be strengthened in an optimal way, leading to a new inequality for which equality can occur, see Corollaries 2.3 and 2.4.

Beyond the realm of random walks on discrete groups, Ledrappier proved that $h \geqslant \ell^2$ for the Brownian motion on the universal cover $\widetilde{M}$ of a compact riemannian manifold M [Led10].

Let μ be a probability measure on the group Γ with a finite first moment, i.e., such that $\sum_g |g|\,\mu(g) < +\infty$ (no symmetry is required). As far as upper bounds for the asymptotic entropy h are concerned, Guivarc'h [Gui80] proved the following so-called "fundamental inequality" between h, ℓ and the growth $v = \lim_n \frac{1}{n} \log \#B(e,n)$ of Γ with respect to S, namely:

$$h \leqslant \ell v.$$

The equality $h = \ell v$ holds in several cases which are well understood, for instance when Γ is the free non-abelian group of rank d and μ is the uniform measure on the canonical set of generators [Led01], or when Γ is a free product of finite groups [MM07]. See also [BHM11] for several characterizations of the equality in terms of quasi-conformal measure on the boundary when Γ is a word-hyperbolic group.

Some contrast appears when one compares the equality $h = \ell v$ and the equality cases in Theorem 1.1. Indeed, we have the following corollaries (which are proved in § 3.4):

Corollary 1.5. *Assume that $\Gamma = \Gamma_1 * \cdots * \Gamma_q$ ($q \geqslant 2$) is a free product of finitely generated groups Γ_i with finite generating sets S_i. Let μ be a symmetric probability measure with support equal to $S = \bigsqcup S_i$. Let A and B be two nondecreasing functions on $[0,1)$ with $A + B \circ G \leqslant F$ such that the equality $A(\ell) + B(1-\rho) = h$ holds. Then the Cayley graph of each Γ_i with respect to S_i is a regular tree (i.e., Γ_i is a free product of finitely many factors $\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$), the Cayley graph of Γ with respect to S is also a regular tree, and μ is the uniform measure on S.*

For instance, consider the modular group $\Gamma = \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z} = \{1, a\} * \{1, b, b^2\}$ and a symmetric probability measure $\mu_p = p\delta_a + \frac{1-p}{2}(\delta_b + \delta_{b^2})$. Then, for all $p \in (0,1)$, one has $h = \ell v$ [MM07] but $A(\ell) + B(1-\rho) < h$.

As far as the free group $\mathbb{F}_d = \mathbb{Z} * \cdots * \mathbb{Z}$ is concerned, the above corollary says that the simple random walk is the only symmetric nearest neighbor random walk for which $A(\ell) + B(1-\rho) = h$ holds.

Let Γ be the fundamental group of a closed compact surface and μ a finitely supported symmetric probability measure on Γ. Deciding whether $h = \ell v$ or $h < \ell v$ is still an open problem, even for the uniform measure on the Poincaré generators of Γ. However, we have the following (see § 3.4):

Corollary 1.6. *Let Γ be a one-ended hyperbolic group and μ a finitely supported symmetric probability measure on Γ whose support generates Γ as a semigroup. Let A and B be two nondecreasing functions on $[0,1)$ such that $A + B \circ G \leqslant F$. Then one has*

$$A(\ell / M_2(\mu)) + B(1-\rho) < h.$$

2. Further results and examples

Our main result, Theorem 1.1, is a consequence of two separate estimates relating the drift (resp. the spectral radius) and the entropy. Those estimates essentially correspond to the endpoints estimates in Theorem 1.1, i.e., $A = 0$ and $B = 0$. However, they are slightly stronger, since they hold under weaker assumptions.

The estimate relating drift and entropy is the following.

Theorem 2.1. *Consider a symmetric random walk on a finitely generated group, with finite first moment. Let ℓ denote its drift, h its entropy, and $M_p(\mu)$ the moment of order p of μ. Then*

$$\sum_{n=1}^{\infty} \frac{2}{2n-1}\left(\frac{\ell}{M_{1+1/(2n-1)}(\mu)}\right)^{2n} \leqslant h.$$

In this theorem, the first terms of the expansion vanish if the corresponding moments are infinite. The theorem gives a nontrivial estimate when μ as a finite moment of some order $p > 1$. In particular, if μ has a moment of order $1 + 1/(2n-1)$, we get

$$\ell \leqslant M_{1+1/(2n-1)}(\mu)\left(\frac{2n-1}{2}h\right)^{1/(2n)}.$$

If $h = 0$ for such a measure, it follows that $\ell = 0$. This is a weak version of a theorem of Karlsson and Ledrappier [KL07], stating that this implication holds for symmetric measures with a finite moment of order 1 (the symmetry assumption can even be replaced by a weaker centering assumption).

Theorem 2.1 is most precise for measures with a finite moment of order 2, since all terms become relevant. Bounding $M_{1+1/(2n-1)}(\mu)$ by $M_2(\mu)$, this yields

$$F\left(\frac{\ell}{M_2(\mu)}\right) \leqslant h, \tag{2.1}$$

thanks to the Taylor expansion of F:

$$F(x) = \sum_{n=1}^{\infty} \frac{2}{2n-1} x^{2n}.$$

This is the special case of Theorem 1.1 corresponding to $A = F$ and $B = 0$.

We now turn to the estimate relating spectral radius and entropy.

Theorem 2.2. *Consider a symmetric random walk on a finitely generated group Γ, with finite entropy h. Let ρ denote its spectral radius. Then*

$$F \circ G^{-1}(1-\rho) \leqslant h.$$

This is the special case of Theorem 1.1 corresponding to $A = 0$ and $B = F \circ G^{-1}$. Note however that there is no moment assumption on μ here, finiteness of the entropy suffices.

The main theorem follows from the above two theorems:

Proof of Theorem 1.1. We have shown in (2.1) that $F(\ell/M_2(\mu)) \leqslant h$, while Theorem 2.2 yields $F \circ G^{-1}(1-\rho) \leqslant h$. Let A and B be nondecreasing functions with $A + B \circ G \leqslant F$, we get

$$A(\ell/M_2(\mu)) + B(1-\rho) \leqslant A \circ F^{-1}(h) + B \circ G \circ F^{-1}(h) = (A + B \circ G)(F^{-1}h) \leqslant F(F^{-1}h) = h.$$

This is the conclusion of Theorem 1.1. □

Corollary 2.3. *Let $A(x) = (1+x)\log(1+x) + (1-x)\log(1-x)$. Then any symmetric random walk with finite second moment satisfies*

$$A(\ell/M_2(\mu)) + 2|\log \rho| \leqslant h.$$

Moreover, equality holds for the simple random walk on the free group.

Indeed, it suffices to take A as in the statement of the corollary and $B(x) = -2\log(1-x)$: those functions are nondecreasing and satisfy $A + B\circ G = F$, hence Theorem 1.1 applies. Surprisingly, for nearest neighbor random walks, we found a direct (and completely different) proof of this result, relying on properties of Chebyshev polynomials and on large deviation estimates for the simple random walk on $\mathbb{Z}$. Since this proof is interesting in its own right, we give it in Appendix A. Note that this statement improves both Avez and Carne-Lœuillot inequalities.

Corollary 2.4. *Let $A(x) = x\log\frac{1+x}{1-x} + 4\sqrt{1-x^2} - 4 \geqslant 0$. Then any symmetric random walk with finite second moment satisfies*

$$A(\ell/M_2(\mu)) + 4(1-\rho) \leqslant h.$$

Moreover, equality holds for the simple random walk on the free group.

This is a first way of improving Ledrappier's inequality $4(1-\rho) \leqslant h$, using the drift ℓ.

Proof. Observe that $A(x) = F(x) - 4G(x)$. Let $B(x) = 4x$. We obviously have $A + B\circ G = F$. In order to apply Theorem 1.1, we have to check that A is nondecreasing. Starting from the Taylor expansions of F and G, we have

$$A(x) = 2\sum_{n=0}^{\infty}\left(\frac{1}{2n+1} - \frac{1}{4^n(n+1)}\binom{2n}{n}\right)x^{2n+2}.$$

For $n \geqslant 1$, one may estimate $(2n)!$ by bounding each odd number in the product by the even number following it. This gives $(2n)! \leqslant 4^n(n!)^2$. Bounding only each odd number > 1 by the even number following it, we even get $(2n)! \leqslant 4^n(n!)^2/2$, hence $4^{-n}\binom{2n}{n} \leqslant 1/2$. Therefore all the coefficients of the Taylor expansion of A are nonnegative, and A is increasing (and nonnegative). □

Theorem 2.2 provides a second way of improving Ledrappier's inequality, using only the spectral radius ρ. We previously need to study more precisely the function $F\circ G^{-1}$. This is done in the next lemma.

Lemma 2.5. *The function $F\circ G^{-1}$ satisfies on $[0,1)$*

$$F\circ G^{-1}(x) = (2x-x^2)^{1/2}\log\left(\frac{1+(2x-x^2)^{1/2}}{1-(2x-x^2)^{1/2}}\right) = \sum_{n=1}^{\infty} c_n x^n,$$

where $c_1 = 4$ and $(2n-1)c_n = (n-2)c_{n-1} + 2$ for $n \geqslant 2$. In particular, the coefficients c_n are positive. Hence, $F\circ G^{-1}$ is increasing and convex.

Proof. A simple computation shows that the function $H = F\circ G^{-1}$ satisfies the differential equation

$$H'(x) = \frac{1-x}{x(2-x)}H(x) + \frac{2}{1-x}.$$

Multiplying by $x(2-x)$ and identifying the Taylor coefficients on the left and on the right, one gets the recurrence relation $(2n-1)c_n = (n-2)c_{n-1} + 2$ for $n \geqslant 2$. □

Corollary 2.6. *Any symmetric random walk with finite entropy satisfies*

$$\sqrt{1-\rho^2}\log\frac{1+\sqrt{1-\rho^2}}{1-\sqrt{1-\rho^2}} = \sum_{n=1}^{\infty} c_n(1-\rho)^n \leqslant h. \tag{2.2}$$

Moreover, equality holds for the simple random walk on the free group.

This is a rephrasing of Theorem 2.2. Obviously, $F\circ G^{-1}(1-\rho)$ is the left hand side in (2.2). This statement is actually an improvement of Ledrappier's inequality since the coefficients c_n are positive.

As another consequence of Theorems 2.1 and 2.2, we get estimates on the drift ℓ, the entropy h and the spectral radius ρ in terms of the growth v of the group Γ.

Corollary 2.7. *Let μ be a symmetric probability measure with a finite second moment on a finitely generated group Γ. Denote by $\tilde{\ell}=\ell/M_2(\mu)$ and $\tilde{v}=M_2(\mu)v$ the drift and the growth for the distance $\tilde{d}(g,h)=d(g,h)/M_2(\mu)$. The following inequalities hold:*

$$\tilde{\ell}\leqslant \tanh(\tilde{v}/2),\quad h\leqslant \tilde{v}\tanh(\tilde{v}/2),\quad \rho\geqslant 1/\cosh(\tilde{v}/2).$$

Again, equalities hold for the simple random walk on the free group.

Proof. The function F satisfies $F(x)=2x\operatorname{argtanh}(x)$. Combining the inequality $F(\tilde{\ell})\leqslant h$ from Theorem 2.1 with the "fundamental inequality" $h\leqslant\tilde{\ell}\tilde{v}$ yields $2\operatorname{argtanh}(\tilde{\ell})\leqslant\tilde{v}$, hence $\tilde{\ell}\leqslant\tanh(\tilde{v}/2)$. Since $h\leqslant\tilde{\ell}\tilde{v}$, we deduce that $h\leqslant\tilde{v}\tanh(\tilde{v}/2)$. Last, we have $F\circ G^{-1}(1-\rho)\leqslant h$. One easily checks that $F\circ G^{-1}(1-1/\cosh(t/2))=t\tanh(t/2)$. Thus Theorem 2.2 implies

$$1-\rho\leqslant G\circ F^{-1}(h)\leqslant G\circ F^{-1}(\tilde{v}\tanh(\tilde{v}/2))=1-1/\cosh(\tilde{v}/2).$$

We get $\rho\geqslant 1/\cosh(\tilde{v}/2)$, as claimed. □

Example. Assume that Γ is the fundamental group of a closed compact surface of genus 2. Consider the following presentation of Γ:

$$\Gamma=\langle a_1,a_2,b_1,b_2\ :\ [a_1,b_1][a_2,b_2]=1\rangle.$$

The growth v of Γ with respect to the generating set $S=\{a_1,a_2,b_1,b_2\}^{\pm1}$ is explicitly known. Following Cannon (see [dlH00]), it is the logarithm of an algebraic number, and its value is $v=1.9430254...$. Let μ be any symmetric probability measure on S. The above corollary yields

$$\ell\leqslant 0.749368278,\quad h\leqslant 1.456041598,\quad \rho\geqslant 0.66215344.$$

Assume now that μ is the uniform measure on S. The best known estimates on ρ are $0.662420\leqslant\rho\leqslant 0.662816$ (see [Bar04] and [Nag97]). The lower bound we obtain for the spectral radius ρ is precise up to $7*10^{-4}$ (although it is less good than Bartholdi's). Using Nagnibeda's upper bound for ρ, the inequality $h\geqslant F\circ G^{-1}(1-\rho)$ gives $h\geqslant 1.452903618$. Since $\ell\geqslant h/v$, we also have $\ell\geqslant 0.747753281$. This proves that the upper bounds we get for ℓ and h are precise up to $2*10^{-3}$ and $4*10^{-3}$.

3. Boundaries, and proofs of the main inequalities

In this section, we prove our two main inequalities, Theorems 2.1 and 2.2. The proof can be equivalently given inside the group (following the ideas of Ledrappier in [Led92]), or using boundaries. We will use the latter point of view, since it allows for more transparent and intrinsic arguments. Moreover, it is more likely to give insights about the equality case in our inequalities.

In this section, Γ will always be a finitely generated group, and μ a symmetric probability measure on Γ whose support generates Γ, with finite entropy.

3.1. **A symmetrization lemma.** Let $(\mathcal{B}, \nu)$ be a probability space endowed with a Γ-action, such that the probability ν is μ-stationary, which means that

$$\nu = \mu * \nu \stackrel{\text{def}}{=} \sum_{\gamma \in \Gamma} \mu(\gamma) \gamma_* \nu.$$

In particular, $\gamma_*\nu$ is absolutely continuous with respect to ν, for every γ in the subgroup generated by the support of μ, which we assume to coincide with Γ.

The Radon-Nikodym cocycle

$$c(\gamma, \xi) = \frac{\mathrm{d}\gamma_*^{-1}\nu}{\mathrm{d}\nu}(\xi)$$

allows us to define a measure on $\Gamma \times \mathcal{B}$:

$$\mathrm{d}m = \frac{1+c}{2}\,\mathrm{d}\mu\,\mathrm{d}\nu.$$

One checks, by means of a change of variables, that m is indeed a probability measure; in fact, for every γ, $\frac{1+c(\gamma,\xi)}{2}\,\mathrm{d}\nu(\xi)$ is a probability measure on $\mathcal{B}$. Moreover, since μ is symmetric, the measure m is invariant under the 'flip' involution $(\gamma, \xi) \mapsto (\gamma^{-1}, \gamma\xi)$.

The following symmetrization lemma will be used several times. The term "symmetrization" comes from the fact the expression on the right-hand-side does not change under the flip involution. It relies crucially on the symmetry of the measure μ.

Lemma 3.1. *Consider an additive cocycle $f : \Gamma \times \mathcal{B} \to \mathbb{R}$, i.e., a function satisfying $f(\gamma\gamma', \xi) = f(\gamma, \gamma'\xi) + f(\gamma', \xi)$. If f is integrable with respect to $\mathrm{d}\mu\,\mathrm{d}\nu$,*

$$\int_{\Gamma\times\mathcal{B}} f(\gamma,\xi)\,\mathrm{d}\mu(\gamma)\,\mathrm{d}\nu(\xi) = \int_{\Gamma\times\mathcal{B}} f(\gamma,\xi)\frac{1-c(\gamma,\xi)}{1+c(\gamma,\xi)}\,\mathrm{d}m(\gamma,\xi).$$

Proof. This easy computation goes as follows. By the change of variable $g = \gamma^{-1}$ and the symmetry of μ, we have

$$\int f(\gamma,\xi)\,\mathrm{d}\mu(\gamma)\,\mathrm{d}\nu(\xi) = \int f(g^{-1},\xi)\,\mathrm{d}\mu(g)\,\mathrm{d}\nu(\xi).$$

The cocycle relation $f(gg', \xi) = f(g, g'\xi) + f(g', \xi)$ implies that $f(g^{-1}, \xi) = -f(g, g^{-1}\xi)$. The change of variable $\eta = g^{-1}\xi$ gives

$$\int f\,\mathrm{d}\mu\,\mathrm{d}\nu = -\int f(g,\eta)\,\mathrm{d}(g_*^{-1}\nu)(\eta)\,\mathrm{d}\mu(g) = \int f\frac{-2c}{1+c}\,\mathrm{d}m.$$

On the other hand, we have of course

$$\int f \,\mathrm{d}\mu \,\mathrm{d}\nu = \int f \frac{2}{1+c} \,\mathrm{d}m.$$

The half-sum of these two relations gives the desired result. □

3.2. **The Poisson boundary, proof of Theorem 2.2.** The proof of Theorem 2.2 relies on the action of (Γ, μ) on its *Poisson boundary* $(\mathcal{B}_0, \nu_0)$. There are several definitions and constructions of this object, see [KV83, Fur02] for details, we will use the entropic characterization 3.1 below. Let c_0, m_0 be the objects defined above, attached to the Poisson boundary.

3.2.1. *A convenient formula for the entropy.* Kaimanovich and Vershik [KV83] proved the following formula for the entropy:

$$h = -\int_{\Gamma\times\mathcal{B}_0} \log c_0 \,\mathrm{d}\mu \,\mathrm{d}\nu_0. \tag{3.1}$$

Since the Radon-Nikodym derivative c_0 is a multiplicative cocycle, the symmetrization lemma 3.1 applies:

$$h = -\int_{\Gamma\times\mathcal{B}_0} \log c_0 \cdot \frac{1-c_0}{1+c_0} \,\mathrm{d}m_0,$$

which can be more conveniently written as

$$h = \int_{\Gamma\times\mathcal{B}_0} F\left(\frac{1-c_0}{1+c_0}\right) \mathrm{d}m_0, \tag{3.2}$$

where F was introduced in (1.1).

3.2.2. *An inequality for the spectral radius.* Recall that a probability measure on a locally compact group is said to be *étalée* if some convolution power of it has a non-singular component with respect to the Haar measure. In the realm of discrete groups, this assumption is automatically satisfied. Thus, by a theorem of Zimmer [Zim78, Cor 5.3], the – ergodic – action of the discrete group Γ on its Poisson boundary is amenable in the sense of Zimmer. The precise definition of this notion will not be important for us, we will only use the following consequence.

Consider the following two unitary representations of Γ: the regular representation π_{reg} defined on $\ell^2(\Gamma)$ by

$$(\pi_{\mathrm{reg}}(\gamma)f)(g) = f(\gamma^{-1}g)$$

and the representation π defined on $L^2(\mathcal{B}_0, \nu_0)$ by

$$(\pi(\gamma)f)(\xi) = c_0(\gamma^{-1}, \xi)^{1/2} f(\gamma^{-1}\xi).$$

Denote by $\pi_{\mathrm{reg}}(\mu)$ and $\pi(\mu)$ the averages of π_{reg} and π with respect to μ, namely:

$$\pi_{\mathrm{reg}}(\mu) = \sum_{\gamma\in\Gamma} \mu(\gamma)\pi_{\mathrm{reg}}(\gamma) \quad \text{and} \quad \pi(\mu) = \sum_{\gamma\in\Gamma} \mu(\gamma)\pi(\gamma).$$

Since the representations π_{reg} and π are unitary and the measure μ is symmetric, the operators $\pi_{\mathrm{reg}}(\mu)$ and $\pi(\mu)$ are self-adjoint.

A theorem of Kuhn [Kuh94] (valid for ergodic amenable actions) implies that the representation π is weakly contained in the regular representation π_{reg}, which means that for every $f \in L^2(\mathcal{B}_0, \nu_0)$, there exists a sequence $\{f_n\}_{n\in\mathbb{N}} \subset \ell^2(\Gamma)$ such that $\lim_n \langle \pi_{\mathrm{reg}}(\gamma) f_n, f_n\rangle = \langle \pi(\gamma) f, f\rangle$ for every $\gamma \in \Gamma$.

We deduce that the operator $\pi(\mu)$ has norm less than or equal to the norm of $\pi_{\mathrm{reg}}(\mu)$, which is, by a result of Kesten [Kes59], exactly the spectral radius ρ. If we consider the scalar product $\langle \pi(\mu)1, 1\rangle$ in $L^2(\mathcal{B}_0, \nu_0)$, we have:

$$\rho = \|\pi_{\mathrm{reg}}(\mu)\| \geqslant \|\pi(\mu)\| \geqslant \langle \pi(\mu)1, 1\rangle = \int_{\Gamma\times\mathcal{B}_0} c_0(\gamma^{-1}, \xi)^{1/2}\, \mathrm{d}\mu\, \mathrm{d}\nu_0 = \int_{\Gamma\times\mathcal{B}_0} c_0^{1/2}\, \mathrm{d}\mu\, \mathrm{d}\nu_0$$

again since the measure μ is symmetric. Therefore,

$$1 - \rho \leqslant 1 - \int_{\Gamma\times\mathcal{B}_0} \frac{2c_0^{1/2}}{1+c_0}\, \mathrm{d}m_0 = \int_{\Gamma\times\mathcal{B}_0} \frac{(1-c_0^{1/2})^2}{1+c_0}\, \mathrm{d}m_0 = \int_{\Gamma\times\mathcal{B}_0} G\left(\frac{1-c_0}{1+c_0}\right) \mathrm{d}m_0,$$

where G was introduced in (1.1).

3.2.3. *Proof of Theorem 2.2.* The map $F \circ G^{-1}$ is increasing, so the above inequality transforms into

$$F \circ G^{-1}(1-\rho) \leqslant F \circ G^{-1}\left(\int_{\Gamma\times\mathcal{B}_0} G\left(\frac{1-c_0}{1+c_0}\right) \mathrm{d}m_0\right). \tag{3.3}$$

Note that the partial inverse G^{-1} of G satisfies $F \circ G^{-1} \circ G = F$ on the interval $(-1, 1)$, because both F and G are even functions. Since $F \circ G^{-1}$ is convex by Lemma 2.5, Jensen's inequality implies that

$$F \circ G^{-1}(1-\rho) \leqslant \int_{\Gamma\times\mathcal{B}_0} F\left(\frac{1-c_0}{1+c_0}\right) \mathrm{d}m_0.$$

By Equation (3.2), this is the required inequality. □

3.3. **The metric compactification, proof of Theorem 2.1.** For the proof of Theorem 2.1, we will need another, more geometric boundary, which will give us access to the metric notion of linear drift, in contrast with the Poisson boundary, which is purely a measure theoretic construction.

We recall the construction of the metric (horospherical) closure of the group G. Let $X \subset \mathbb{R}^\Gamma$ be the set of 1-Lipschitz real-valued functions on Γ which vanish on e. Lipschitz means here that $|\varphi(gg') - \varphi(g)| \leqslant |g'|$. For any $\gamma \in \Gamma$,

$$\Phi_\gamma(g) = \left|\gamma^{-1} g\right| - \left|\gamma^{-1}\right|$$

defines an element of X, and the assignment $\gamma \mapsto \Phi_\gamma$ is continuous, injective. Let $\mathcal{B}_1$ be the closure of the image of Γ. The action of Γ on $\mathcal{B}_1$ is given by

$$(\gamma\xi)(g) = \xi(\gamma^{-1} g) - \xi(\gamma^{-1}).$$

The latter equation for the action is better understood if one thinks of X as the quotient set of 1-Lipschitz functions on Γ modulo the constants, endowed with the natural translation action on functions. Each element of X has a unique representative which vanishes at e, which explains the above formula.

3.3.1. *Symmetrized Furstenberg-Khasminskii Formula for the linear drift.* Karlsson and Ledrappier [KL07], [KL11, Thm 18] proved that in this setting, under the assumption of finite first moment, there exists an ergodic stationary probability measure ν_1 on $\mathcal{B}_1$, which satisfies the Furstenberg-Khasminskii formula:

$$\ell = \int_{\Gamma\times\mathcal{B}_1} \xi(\gamma^{-1})\,\mathrm{d}\mu(\gamma)\,\mathrm{d}\nu_1(\xi).$$

By definition of the action, the assignment $\beta : (g,\xi) \mapsto \xi(g^{-1})$ satisfies

$$\beta(gg',\xi) = \xi(g'^{-1}g^{-1}) = (g'\xi)(g^{-1}) + \xi(g'^{-1}) = \beta(g, g'\xi) + \beta(g',\xi),$$

so it is an additive cocycle; this is in fact the classical Busemann cocycle. Hence, the symmetrization lemma 3.1 applies, and we find

$$\ell = \int_{\Gamma\times\mathcal{B}_1} \beta\cdot\frac{1-c_1}{1+c_1}\,\mathrm{d}m_1, \tag{3.4}$$

where c_1 and m_1 denote the Radon-Nikodym derivative and the measure $\frac{1+c_1}{2}\,\mathrm{d}\mu\,\mathrm{d}\nu_1$ respectively, as in the case of the Poisson boundary.

3.3.2. *An inequality for the entropy.* We consider the notion, introduced by Furstenberg, of boundary entropy, in the case of the metric compactification endowed with the measure ν_1. This is by definition the following number:

$$h_\mu(\mathcal{B}_1,\nu_1) = -\int_{\Gamma\times\mathcal{B}_1} \log c_1\ \mathrm{d}\mu\,\mathrm{d}\nu_1.$$

Kaimanovich and Vershik [KV83] proved that the boundary entropy of a space endowed with a stationary measure is always less than or equal to the entropy of the random walk. Hence, by the symmetrization lemma 3.1, we have

$$h \geqslant h_\mu(\mathcal{B}_1,\nu_1) = \int_{\Gamma\times\mathcal{B}_1} F\left(\frac{1-c_1}{1+c_1}\right)\mathrm{d}m_1.$$

3.3.3. *Proof of Theorem 2.1.* Let $n \geqslant 1$ be an integer. Using Hölder's inequality in Equation (3.4) for the exponent $1+1/(2n-1)$ and the conjugate exponent $2n$, the drift ℓ satisfies

$$\ell \leqslant \left(\int_{\Gamma\times\mathcal{B}_1} |\beta|^{1+1/(2n-1)}\,\mathrm{d}m_1\right)^{(2n-1)/(2n)} \left(\int_{\Gamma\times\mathcal{B}_1} \left(\frac{1-c_1}{1+c_1}\right)^{2n}\mathrm{d}m_1\right)^{1/(2n)}. \tag{3.5}$$

Since $|\beta(g,\xi)| \leqslant |g|$, because $\mathcal{B}_1$ consists of 1-Lipschitz functions vanishing at e,

$$\int_{\Gamma\times\mathcal{B}_1} |\beta|^{1+1/(2n-1)}\,\mathrm{d}m_1 \leqslant \int_\Gamma |\gamma|^{1+1/(2n-1)}\left(\int_{\mathcal{B}_1}\frac{1+c_1(\gamma,\xi)}{2}\,\mathrm{d}\nu_1(\xi)\right)\mathrm{d}\mu(\gamma). \tag{3.6}$$

For each γ, the measure on $\mathcal{B}_1$ given by $\frac{1+c_1(\gamma,\xi)}{2}\,\mathrm{d}\nu_1(\xi)$ is a probability measure. Thus,

$$\left(\frac{\ell}{M_{1+1/(2n-1)}(\mu)}\right)^{2n} \leqslant \int_{\Gamma\times\mathcal{B}_1}\left(\frac{1-c_1}{1+c_1}\right)^{2n}\mathrm{d}m_1.$$

Note that the previous equation makes sense even if μ has no finite moment of order $1+1/(2n-1)$ (in this case, the left hand size vanishes, and the equation is trivial). The point

here is that if μ has a finite moment of order $1+\varepsilon$ for some $\varepsilon > 0$, this will give a nontrivial result for some $n \geqslant 1$.

Multiplying this inequality by $2/(2n-1)$ and summing over n, we obtain

$$\begin{aligned}\sum_{n\geqslant 1} \frac{2}{2n-1}\left(\frac{\ell}{M_{1+1/(2n-1)}(\mu)}\right)^{2n} &\leqslant \int_{\Gamma\times\mathcal{B}_1} \sum_{n\geqslant 1} \frac{2}{2n-1}\left(\frac{1-c_1}{1+c_1}\right)^{2n} \mathrm{d}m_1 \\ &= \int_{\Gamma\times\mathcal{B}_1} F\left(\frac{1-c_1}{1+c_1}\right) \mathrm{d}m_1 = h_\mu(\mathcal{B}_1,\nu_1) \leqslant h\end{aligned}$$

as claimed. □

3.4. **Discussion of the equality case.** The proofs given in the previous paragraphs imply that the equality situation in those inequalities is very rigid:

Proposition 3.2. *Consider a symmetric measure μ on a countable group Γ, with finite second moment. Assume that, for some nondecreasing functions A and B with $A+B\circ G \leqslant F$, equality holds in Theorem 1.1, i.e., $A(\ell/M_2(\mu)) + B(1-\rho) = h$. Then, on the Poisson boundary $(\mathcal{B}_0, \nu_0)$ of (Γ,μ), the Radon-Nikodym cocycle $c_0(\gamma,\xi)$ takes only two values e^{α} and $\mathrm{e}^{-\alpha}$, $\mu\otimes\nu_0$ almost surely.*

Proof. If equality holds in Theorem 1.1, then equality has to hold at least at one of the two endpoint inequalities, i.e., for $A = F$ or for $B\circ G = F$.

Assume first that $F\circ G^{-1}(1-\rho) = h$. Then all the inequalities in the proof of Theorem 2.2 have to be equalities. In particular, Jensen's inequality after (3.3) is an equality, whence $G((1-c_0)/(1+c_0))$ is almost surely constant, i.e., there exists $a\in\mathbb{R}$ such that $(1-c_0)/(1+c_0) = \pm a$ almost surely. Hence, $c_0 = (1-b)/(1+b)$ for $b = \pm a$. This shows that c_0 takes only two values, which are inverse one of each other.

Assume now that $F(\ell/M_2(\mu)) = h$. Denote by $(\mathcal{B}_1,\nu_1)$ the metric compactification used in Paragraph 3.3. We have the inequalities

$$\begin{aligned}(3.7)\quad F\left(\frac{\ell}{M_2(\mu)}\right) &= \sum \frac{2}{2n-1}\left(\frac{\ell}{M_2(\mu)}\right)^{2n} \\ &\leqslant \sum \frac{2}{2n-1}\left(\frac{\ell}{M_{1+1/(2n-1)}(\mu)}\right)^{2n} \leqslant h_\mu(\mathcal{B}_1,\nu_1) \leqslant h.\end{aligned}$$

If the extreme terms are equal, we have equality everywhere.

All the moments of μ coincide, hence μ is supported on points at a fixed distance of e. Since equality has to hold in (3.6), we also deduce that $|\beta(\gamma,\xi)| = |\gamma|$ almost surely. This implies that $|\beta|$ is almost surely constant. Finally, there is equality in the Hölder inequality (3.5), hence, $(1-c_1)/(1+c_1)$ is almost surely proportional to β. It follows that $|(1-c_1)/(1+c_1)|$ is almost surely constant. Hence, as in the first case, c_1 takes only two values which are inverse of each other. To conclude, we should prove that this property (that we have proved on $(\mathcal{B}_1,\nu_1)$) also holds on the Poisson boundary.

Since equality holds everywhere in (3.7), one has in particular $h_\mu(\mathcal{B}_1,\nu_1) = h$. By [KV83, Theorem 3.2], this implies that $(\mathcal{B}_1,\nu_1)$ is the Poisson boundary if the Radon-Nikodym cocycle separates the points, i.e., if for almost every points $\xi\neq\eta$ there exists $g\in\Gamma$ such that $c_1(g,\xi)\neq c_1(g,\eta)$. In general, the Poisson boundary is a factor of $(\mathcal{B}_1,\nu_1)$, obtained by

identifying the points that are not separated by the Radon-Nikodym cocycle. In particular, any property of the Radon-Nikodym cocycle that is true on $(\mathcal{B}_1, \nu_1)$ is also true on the Poisson boundary. This concludes the proof. $\square$

We now have the tools to prove Corollaries 1.5 and 1.6, that we restate for clarity.

Corollary 1.5. *Assume that $\Gamma = \Gamma_1 * \cdots * \Gamma_q$ ($q \geqslant 2$) is a free product of finitely generated groups Γ_i with finite generating sets S_i. Let μ be a symmetric probability measure with support equal to $S = \bigsqcup S_i$. Let A and B be two nondecreasing functions on $[0, 1)$ with $A + B \circ G \leqslant F$ such that the equality $A(\ell) + B(1 - \rho) = h$ holds. Then the Cayley graph of each Γ_i with respect to S_i is a regular tree (i.e., Γ_i is a free product of finitely many factors $\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$), the Cayley graph of Γ with respect to S is also a regular tree, and μ is the uniform measure on S.*

Proof. For $u \in \Sigma = \bigsqcup \Gamma_i \setminus \{e\}$, write $\overline{u} = i$ if $u \in \Gamma_i$. A – finite or infinite – word $u_1 u_2 \cdots$ over the alphabet Σ is *reduced* if $\overline{u_i} \neq \overline{u_{i+1}}$. The group Γ is the set of finite reduced words over Σ (the identity is the empty word) endowed with the internal law which is the concatenation with possible simplification at the contact point. Denote by $|\cdot|_i$ the word metric on Γ_i associated to S_i. The word metric $|\cdot|$ on Γ with respect to $S = \bigsqcup S_i$ is then given by $|u| = |u|_{\overline{u}}$ if $u \in \Sigma$, and $|u| = |u_1| + \cdots + |u_k|$ if $u = u_1 \cdots u_k$ is reduced over Σ.

Denote by $\mathcal{E}(\Gamma)$ the *space of ends* of Γ. Let μ be a symmetric probability measure on Γ with support equal to S. Then there exists a unique probability measure ν on $\mathcal{E}(\Gamma)$ which is μ-stationary, and the space $(\mathcal{E}(\Gamma), \nu)$ is (a realization of) the Poisson boundary of (Γ, μ) (see [Woe89, Woe93] and also [Kai00]). The set $\partial\Gamma$ of right infinite reduced words $\xi = \xi_1 \xi_2 \cdots$ over Σ is a Γ-invariant subset of $\mathcal{E}(\Gamma)$ with full ν-measure.

For $a \in \Gamma$, denote by $q(a) = \mathbf{P}(\exists n, X_n = a)$ the probability that the random walk ever reaches a. For $a \in \Sigma$ and $\xi = \xi_1 \xi_2 \cdots \in \partial\Gamma$, we have

$$c(a, \xi) = \begin{cases} q(a) & \text{if } \overline{\xi_1} \neq \overline{a} \\ q(a\xi_1)/q(\xi_1) & \text{if } \overline{\xi_1} = \overline{a} \end{cases}, \tag{3.8}$$

see [DM61], [Led01] and [MM07].

Assume that the equality $A(\ell) + B(1 - \rho) = h$ holds. Proposition 3.2 provides a real number $\alpha \geqslant 0$ such that $c(a, \xi) \in \{e^{\alpha}, e^{-\alpha}\}$ for $\mu \otimes \nu$-almost every $(a, \xi) \in \Sigma \times \partial\Gamma$. Since $q(a) < 1$ as the random walk on a free product is transient, Equation (3.8) implies that $\alpha > 0$ and $q(a) = e^{-\alpha}$ for all $a \in S$.

Consider two elements $a, b \in S_i$ (possibly with $a = b$), with $ab \neq e$. The second case in (3.8) shows that $q(ab)/q(b) \in \{e^{\alpha}, e^{-\alpha}\}$. Since $q(b) = e^{-\alpha}$, this gives $q(ab) \in \{1, e^{-2\alpha}\}$. Since $ab \neq e$ and the random walk is transient, we have $q(ab) < 1$, hence $q(ab) = e^{-2\alpha}$. This gives

$$\begin{aligned} \mathbf{P}(\exists m < n, X_m = a, X_n = ab) &= \mathbf{P}(\exists m, X_m = a)\mathbf{P}(\exists n, X_n = b) = q(a)q(b) \\ &= e^{-2\alpha} = q(ab) = \mathbf{P}(\exists n, X_n = ab), \end{aligned}$$

where we used the Markov property for the first equality. This shows that almost every path from e to ab has to pass first through a. Equivalently, whenever we write ab as a product $s_1 \ldots s_n$ of elements of S_i, then some prefix $s_1 \ldots s_m$ is equal to a.

This implies that there is no nontrivial loop in the Cayley graph of Γ_i with respect to S_i: if there were such an injective loop $e, a_1, a_1a_2, \dots, a_1a_2\cdots a_{k-1}, a_1a_2\cdots a_{k-1}a_k = e$ (where all points but the first and last one are distinct), then $a_1a_2 = (a_3\cdots a_k)^{-1} = a_k^{-1}\cdots a_3^{-1}$. Since S_i is symmetric, we have written a_1a_2 as a product of elements of S_i that never reaches a_1 (since the loop is injective), a contradiction. This shows that the Cayley graph of Γ_i with respect to S_i is a regular tree, and therefore that Γ_i is a free product of finitely many factors $\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$.

The Cayley graph of Γ with respect to S is also a regular tree. Since the probabilities of ever reaching any neighbor of the origin are the same, so are the transition probabilities, hence μ is uniform on Σ. □

Corollary 1.6. *Let Γ be a one-ended hyperbolic group and μ a finitely supported symmetric probability measure on Γ whose support generates Γ as a semigroup. Let A and B be two nondecreasing functions on $[0,1)$ such that $A + B\circ G \leqslant F$. Then one has*

$$A(\ell/M_2(\mu)) + B(1-\rho) < h.$$

Proof. Let Γ be a one-ended hyperbolic group. If μ is a finitely supported probability measure on Γ, then it follows from [Anc88] that the Poisson boundary and the the Martin boundary of (Γ,μ) can be identified with $(\partial\Gamma,\nu)$ where $\partial\Gamma$ is the geometric boundary of Γ and ν is the unique μ-stationary measure on $\partial\Gamma$. In particular, the Poisson boundary is endowed with the topology of $\partial\Gamma$ for which it is a connected space. Moreover, the trivial continuity of the Martin kernel $K(g,\xi)$ implies the continuity of the Radon-Nikodym cocycle $c_0(g,\xi)$ since $c_0 = \log K$.

Assume that the equality $A(\ell/M_2(\mu)) + B(1-\rho) = h$ holds. From Proposition 3.2, the continuous function $\xi \mapsto c_0(g,\xi)$ can only take two values for g in the support of μ. Since the Poisson boundary is connected, this function has to be constant. In particular, the map $\xi \mapsto g\xi$ has a constant jacobian, which must be equal to 1 since this transformation maps a probability measure to a probability measure. Therefore, $c_0(g,\xi) = 0$, which yields $h = 0$ thanks to the formula (3.1). This is a contradiction since Γ is non-amenable, hence $h > 0$. □

From the free group, one can construct other examples where equality holds in Theorem 1.1. For instance, let H be a finite group and let $\mathbb{F}$ be a free group on finitely many generators $\{a_1,\dots,a_d\}$. In $\Gamma = \mathbb{F}\times H$, consider the generating set $S = \{(a_i^{\pm 1}, x) : i \in \{1,\dots,d\}, x \in H\}$. The simple random walk on (Γ, S) projects to the simple random walk on the free factor $\mathbb{F}$, and those random walks have the same drift, entropy and spectral radius. Since equality holds in Theorem 1.1 for $\mathbb{F}$, it follows that is also holds for (Γ, S).

More generally, consider an exact sequence $1 \to H \to \Gamma \to \mathbb{F} \to 1$ where $\mathbb{F}$ is a group whose Cayley graph is a tree, and a probability measure on the set of generators of Γ that projects to the uniform measure on the generators of $\mathbb{F}$. If the drift, entropy and spectral radius of the random walk on Γ are the same as on $\mathbb{F}$ (this is for instance the case if H has subexponential growth), then equality holds in Theorem 1.1 for the random walk on Γ. We conjecture (but are unable to prove) that this is the only case where equality holds in this theorem.

Appendix A. An elementary proof of Corollary 2.3 for nearest-neighbor random walks

In this appendix, we give another completely different proof of Corollary 2.3 in the special case of nearest-neighbor random walks. This proof is inspired by the techniques of Carne [Car85]. We will always write A for the function in the statement of the corollary, i.e., $A(x) = (1+x)\log(1+x) + (1-x)\log(1-x)$. Recall that Γ is a finitely generated group, S is a finite symmetric generating system of Γ and μ is a symmetric probability measure on S. We want to prove that

$$A(\ell) + 2\,|\log \rho| \leqslant h.$$

Consider the Hilbert space $\ell^2(\Gamma)$, with its scalar product $\langle \cdot, \cdot \rangle$. The Markov operator P_μ associated to μ is defined by $P_\mu f(g) = \sum_{h\in\Gamma} \mu(h) f(gh)$. It is a contraction on $\ell^2(\Gamma)$, and its iterates are given by $P_\mu^n = P_{\mu^{*n}}$.

Since the measure μ is symmetric, the operator P_μ is self-adjoint, therefore its spectrum $\sigma(P_\mu)$ is real and contained in the interval $[-1, 1]$. Moreover, the spectral radius of P_μ is given by

$$\rho(P_\mu) = \sup_{\lambda\in\sigma(P_\mu)} |\lambda| = \|P_\mu\| = \rho.$$

The second equality holds for every self-adjoint operator. See [Kes59] for the last equality.

If $K \subset \Gamma$, we write $\mathbb{I}_K$ for the indicator function of K. It belongs to $\ell^2(\Gamma)$ when K is finite. If $K = \{g\}$, we simply write $\mathbb{I}_g$. We have, for every $g \in \Gamma$,

$$\langle P_\mu^n \mathbb{I}_e, \mathbb{I}_g \rangle = (P_\mu^n \mathbb{I}_e)(g) = \sum_{h\in\Gamma} \mu^{*n}(h)\mathbb{I}_e(gh) = \mu^{*n}(g^{-1}) = \mu^{*n}(g)$$

since μ is symmetric. More generally, for every $K \subset \Gamma$,

$$\langle P_\mu^n \mathbb{I}_e, \mathbb{I}_K \rangle = \mu^{*n}(K).$$

Lemma A.1. *Let $(T_k(X))_k$ be the sequence of Chebyshev polynomials and let $(S_n)_n$ be the simple random walk on $\mathbb{Z}$. Then:*

1. *for every $n \in \mathbb{N}$, one has $X^n = \sum_{k=0}^n \mathbf{P}(|S_n| = k) T_k(X)$;*
2. *for every self-adjoint operator u of a Hilbert space with unit norm, $\|T_k(u)\| = 1$ for all $k \in \mathbb{N}$;*
3. *for every $k, n \in \mathbb{N}$ such that $0 \leqslant k \leqslant n$, one has $\mathbf{P}(S_n \geqslant k) \leqslant \exp\big[-\frac{n}{2} A\big(k/n\big)\big]$.*

Proof. (1) This is [Car85, Thm. 2]. We recall Carne's proof in order to be complete. Set $x = \cos t$. Then:

$$\begin{aligned} x^n &= \frac{1}{2^n}\big(e^{it} + e^{-it}\big)^n = \sum_{k=-n}^{n} \mathbf{P}(S_n = k) e^{ikt} = \sum_{k=0}^{n} \mathbf{P}(|S_n| = k) \frac{e^{ikt} + e^{-ikt}}{2} \\ &= \sum_{k=0}^{n} \mathbf{P}(|S_n| = k) \cos kt = \sum_{k=0}^{n} \mathbf{P}(|S_n| = k) T_k(\cos t) = \sum_{k=0}^{n} \mathbf{P}(|S_n| = k) T_k(x). \end{aligned}$$

(2) The Chebyshev polynomials satisfy $T_k([-1, 1]) = [-1, 1]$ and $|T_k(\pm 1)| = 1$. Moreover, since T_k is real and u self-adjoint, the operator $T_k(u)$ is also self-adjoint. If $\|u\| = 1$, then

$\sigma(u) \subset [-1,1]$, hence $\sigma(T_k(u)) = T_k(\sigma(u)) \subset [-1,1]$. We have

$$\|T_k(u)\| = \sup\{|\lambda|\,, \lambda \in \sigma(T_k(u))\} = \sup\{|T_k(\lambda)|\,, \lambda \in \sigma(u)\} = 1.$$

(3) This is a standard Chernov type estimate. For every real $t > 0$, we have, using Markov inequality,

$$\mathbf{P}(S_n \geqslant k) = \mathbf{P}(e^{tS_n} \geqslant e^{tk}) \leqslant e^{-tk}\mathbf{E}(e^{tS_n}) = e^{-tk}(\cosh t)^n = \exp\left[-n\left(t\frac{k}{n} - \log\cosh t\right)\right].$$

An elementary computation shows that, for $x \in [0,1]$, $\sup\{tx - \log\cosh t, t > 0\} = A(x)/2$. The result follows. Observe that the function A appears as twice the Legendre transform of the function $\log\cosh$, hence is convex. □

Recall that, for every $K \subset \Gamma$, we have $\mu^{*n}(K) = \langle P_\mu^n \mathbb{I}_e, \mathbb{I}_K\rangle$. Applying Item (1) of lemma A.1, we get

$$\frac{1}{\rho^n}\mu^{*n}(K) = \left\langle \left(\frac{1}{\rho}P_\mu\right)^n \mathbb{I}_e, \mathbb{I}_K \right\rangle = \sum_{k=0}^{n} \mathbf{P}(|S_n| = k) \left\langle T_k\left(\frac{1}{\rho}P_\mu\right)\mathbb{I}_e, \mathbb{I}_K \right\rangle. \tag{A.1}$$

What remains to do is to apply this formula to a suitable sequence of finite subsets of Γ. Fix $\varepsilon > 0$. Let $K_n \subset \Gamma$ be defined by

$$K_n = \{g \in \Gamma \,:\, |g| \in [\ell(1-\varepsilon)n, \ell(1+\varepsilon)n] \text{ and } \mu^{*n}(g) \in [e^{-h(1+\varepsilon)n}, e^{-h(1-\varepsilon)n}]\}.$$

Recall that we denote by $(X_n)_n$ (a realization of) the right random walk associated with (Γ, μ). Using Kingman's subadditive ergodic theorem [Der80], one can prove that, as $n \to +\infty$, $|X_n|/n \to \ell$ and $-\log\mu^{*n}(X_n)/n \to h$ almost surely, hence in probability. Therefore, $\lim_n \mu^{*n}(K_n) = 1$. In particular, taking n large enough, one has $\mu^{*n}(K_n) \geqslant 1 - \varepsilon$.

Denote by $\#K$ the cardinality of a set $K \subset \Gamma$. We have

$$1 \geqslant \mu^{*n}(K_n) \geqslant \#K_n e^{-h(1+\varepsilon)n},$$

hence $\#K_n \leqslant e^{h(1+\varepsilon)n}$.

Observe that, since $\deg T_k = k$ and $\mathrm{supp}(\mu) \subset S$, the support of the function $T_k\left(\frac{1}{\rho}P_\mu\right)\mathbb{I}_e$ is contained in the ball $B(e,k)$, and therefore is disjoint from the support of the function $\mathbb{I}_{K_n}$ if $k < \ell(1-\varepsilon)n$. The identity (A.1) written with the set K_n then becomes

$$\frac{1}{\rho^n}\mu^{*n}(K_n) = \sum_{\ell(1-\varepsilon)n \leqslant k \leqslant n} \mathbf{P}(|S_n| = k)\left\langle T_k\left(\frac{1}{\rho}P_\mu\right)\mathbb{I}_e, \mathbb{I}_{K_n}\right\rangle.$$

Using Cauchy-Schwarz inequality and the item (2) of lemma A.1, we obtain

$$\begin{aligned}
\frac{1}{\rho^n}\mu^{*n}(K_n) &\leqslant \sum_{\ell(1-\varepsilon)n \leqslant k \leqslant n} \mathbf{P}(|S_n| = k)\left\|T_k\left(\frac{1}{\rho}P_\mu\right)\right\| \cdot \|\mathbb{I}_e\|_2 \cdot \|\mathbb{I}_{K_n}\|_2 \\
&\leqslant \mathbf{P}(|S_n| \geqslant \ell(1-\varepsilon)n)\sqrt{\#K_n} \\
&\leqslant 2\mathbf{P}(S_n \geqslant \ell(1-\varepsilon)n)\sqrt{e^{h(1+\varepsilon)n}}.
\end{aligned}$$

The item (3) of lemma A.1 yields

$$\frac{1-\varepsilon}{\rho^n} \leqslant \frac{1}{\rho^n}\mu^{*n}(K_n) \leqslant 2\exp\left[-\frac{n}{2}A(\ell(1-\varepsilon)) + \frac{1}{2}h(1+\varepsilon)n\right].$$

Taking the logarithm of both sides and dividing by n gives

$$\frac{\log(1-\varepsilon)}{n} - \log\rho \leqslant \frac{\log 2}{n} - \frac{1}{2}A(\ell(1-\varepsilon)) + \frac{1}{2}h(1+\varepsilon).$$

Letting $n \to +\infty$ and $\varepsilon \to 0$ we get $-\log\rho \leqslant -A(\ell)/2 + h/2$. This concludes this proof of the corollary for nearest-neighbor random walks. □

Remark A.2. Let μ be a symmetric probability measure on Γ supported in the generating set S. Writing equation (A.1) for $K = \{g\}$ and following the above proof leads to

$$\frac{1}{\rho^n}\mu^{*n}(g) = \sum_{k=|g|}^{n} \mathbf{P}(|S_n| = k)\left\langle T_k\left(\frac{1}{\rho}P_\mu\right)\mathbb{I}_e, \mathbb{I}_g\right\rangle \leqslant \mathbf{P}(|S_n| \geqslant |g|).$$

Therefore we have

$$\mu^{*n}(g) \leqslant 2\rho^n\mathbf{P}(S_n \geqslant |g|) \leqslant 2\rho^n \exp\left[-\frac{n}{2}A\left(\frac{|g|}{n}\right)\right],$$

which is Lœuillot's upper bound for $\mu^{*n}(g)$ (see [Lœu11]). It is also possible to get *lower* bounds for $\mu^{*n}(g)$ using lemma A.1, see [Woe00, Thm. 14.22].

Remark A.3. As Peter Haïssinsky kindly pointed out to us, a very short proof of the "fundamental inequality" $h \leqslant \ell v$ can be obtained using the sets K_n. It relies on the fact that, on K_n, $\mu^{*n}(g) \leqslant e^{-h(1-\varepsilon)n}$ and $|g| \leqslant \ell(1+\varepsilon)n$.

We have

$$1-\varepsilon \leqslant \mu^{*n}(K_n) \leqslant \#K_n e^{-h(1-\varepsilon)n}$$

therefore

$$(1-\varepsilon)e^{h(1-\varepsilon)n} \leqslant \#K_n \leqslant \#B(e, \ell(1+\varepsilon)n).$$

Taking the logarithm of both sides and dividing by n gives

$$\frac{\log(1-\varepsilon)}{n} + h(1-\varepsilon) \leqslant \ell(1+\varepsilon) \times \frac{1}{\ell(1+\varepsilon)n}\log\#B(e, \ell(1+\varepsilon)n).$$

Letting $n \to +\infty$ and $\varepsilon \to 0$ yields $h \leqslant \ell v$.

Acknowledgements: The authors gladly thank Bachir Bekka for pointing out to them the references [Zim78] and [Kuh94], and Peter Haïssinsky for letting them reproduce the above short proof of the fundamental inequality.

References

[Anc88] Alano Ancona, *Positive harmonic functions and hyperbolicity*, Potential theory, surveys and problems (Prague, 1987), Lecture Notes in Math., vol. 1344, Springer, Berlin, 1988, pp. 1–23. MR973878. Cited page 14.

[Ave76] André Avez, *Croissance des groupes de type fini et fonctions harmoniques*, Théorie ergodique (Actes Journées Ergodiques, Rennes, 1973/1974), Springer, Berlin, 1976, pp. 35–49. Lecture Notes in Math., Vol. 532. MR0482911. Cited page 2.

[Bar04] Laurent Bartholdi, *Cactus trees and lower bounds on the spectral radius of vertex-transitive graphs*, Random walks and geometry, Walter de Gruyter GmbH & Co. KG, Berlin, 2004, pp. 349–361. MR2087788. Cited page 7.

[BHM11] Sébastien Blachère, Peter Haïssinsky, and Pierre Mathieu, *Harmonic measures versus quasiconformal measures for hyperbolic groups*, Ann. Sci. Éc. Norm. Supér. (4) **44** (2011), 683–721. MR2919980. Cited page 4.

[Car85] Thomas Keith Carne, *A transmutation formula for Markov chains*, Bull. Sci. Math. (2) **109** (1985), 399–405. MR837740. Cited pages 3 and 15.

[Der80] Yves Derriennic, *Quelques applications du théorème ergodique sous-additif*, Conference on Random Walks (Kleebach, 1979) (French), Astérisque, vol. 74, Soc. Math. France, Paris, 1980, pp. 183–201. MR588163. Cited page 16.

[Der86] Y. Derriennic, *Entropie, théorèmes limite et marches aléatoires*, Probability measures on groups, VIII (Oberwolfach, 1985), Lecture Notes in Math., vol. 1210, Springer, Berlin, 1986, pp. 241–284. 879010 (89f:60076b). Cited page 2.

[dlH00] Pierre de la Harpe, *Topics in geometric group theory*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 2000. MR1786869. Cited page 7.

[DM61] Evgeniĭ B. Dynkin and Mikhail B. Maljutov, *Random walk on groups with a finite number of generators*, Dokl. Akad. Nauk SSSR **137** (1961), 1042–1045. MR0131904. Cited page 13.

[EK12] Anna Erschler and Anders Kalrsson, *Homomorphismes to $\mathbb{R}$ constructed from random walks*, preprint, 2012. Cited page 3.

[Fur02] Alex Furman, *Random walks on groups and random transformations*, Handbook of dynamical systems, Vol. 1A, North-Holland, Amsterdam, 2002, pp. 931–1014. MR1928529. Cited page 9.

[Gui80] Yves Guivarc'h, *Sur la loi des grands nombres et le rayon spectral d'une marche aléatoire*, Conference on Random Walks (Kleebach, 1979) (French), Astérisque, vol. 74, Soc. Math. France, Paris, 1980, pp. 47–98, 3. MR588157. Cited page 4.

[Kai98] Vadim A. Kaimanovich, *The Poisson formula for groups with hyperbolic properties*, Preliminary version of the paper in Ann. of Maths. (1998), Preprint arXiv:math/9802132v1. Cited page 2.

[Kai00] ———, *The Poisson formula for groups with hyperbolic properties*, Ann. of Math. (2) **152** (2000), 659–692. MR1815698. Cited page 13.

[Kes59] Harry Kesten, *Symmetric random walks on groups*, Trans. Amer. Math. Soc. **92** (1959), 336–354. MR0109367. Cited pages 10 and 15.

[KL07] Anders Karlsson and François Ledrappier, *Linear drift and Poisson boundary for random walks*, Pure Appl. Math. Q. **3** (2007), 1027–1036. MR2402595. Cited pages 5 and 11.

[KL11] ———, *Noncommutative ergodic theorems*, Geometry, rigidity, and group actions, Chicago Lectures in Math., Univ. Chicago Press, Chicago, IL, 2011, pp. 396–418. MR2807838. Cited page 11.

[Kuh94] M. Gabriella Kuhn, *Amenable actions and weak containment of certain representations of discrete groups*, Proc. Amer. Math. Soc. **122** (1994), 751–757. MR1209424. Cited pages 9 and 17.

[KV83] Vadim A. Kaĭmanovich and Anatoly M. Vershik, *Random walks on discrete groups: boundary and entropy*, Ann. Probab. **11** (1983), 457–490. MR704539. Cited pages 9, 11, and 12.

[Led92] François Ledrappier, *Sharp estimates for the entropy*, Harmonic analysis and discrete potential theory (Frascati, 1991), Plenum, New York, 1992, pp. 281–288. MR1222466. Cited pages 3 and 8.

[Led01] ———, *Some asymptotic properties of random walks on free groups*, Topics in probability and Lie groups: boundary theory, CRM Proc. Lecture Notes, vol. 28, Amer. Math. Soc., Providence, RI, 2001, pp. 117–152. MR1832436. Cited pages 4 and 13.

[Led10] ———, *Linear drift and entropy for regular covers*, Geom. Funct. Anal. **20** (2010), 710–725. MR2720229. Cited page 3.

[Lœu11] Julien Lœuillot, *Entropie asymptotique, rayon spectral et vitesse de fuite des marches aléatoires dans les groupes*, Mémoire de Master Recherche, Univ. Nantes, 2011. Cited pages 3 and 17.

[MM07] Jean Mairesse and Frédéric Mathéus, *Random walks on free products of cyclic groups*, J. Lond. Math. Soc. (2) **75** (2007), 47–66. MR2302729. Cited pages 4 and 13.

[Nag97] Tatyana Nagnibeda, *An upper bound for the spectral radius of a random walk on surface groups*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **240** (1997), 154–165, 293–294. MR1691645. Cited page 7.

[Var85] Nicholas Th. Varopoulos, *Long range estimates for Markov chains*, Bull. Sci. Math. (2) **109** (1985), 225–252. MR822826. Cited page 3.

[Woe89] Wolfgang Woess, *Boundaries of random walks on graphs and groups with infinitely many ends*, Israel J. Math. **68** (1989), 271–301. MR1039474. Cited page 13.

[Woe93] ———, *Fixed sets and free subgroups of groups acting on metric spaces*, Math. Z. **214** (1993), 425–439. MR1245204. Cited page 13.

[Woe00] ———, *Random walks on infinite graphs and groups*, Cambridge Tracts in Mathematics, vol. 138, Cambridge University Press, Cambridge, 2000. MR1743100. Cited page 17.

[Zim78] Robert J. Zimmer, *Amenable ergodic group actions and an application to Poisson boundaries of random walks*, J. Functional Analysis **27** (1978), 350–372. MR0473096. Cited pages 9 and 17.

Sébastien Gouëzel, IRMAR, Université Rennes 1, 35042 Rennes Cedex, France
E-mail address: `sebastien.gouezel@univ-rennes1.fr`

Frédéric Mathéus, Université de Bretagne Sud, L.M.B.A., UMR 6205, BP 573, 56017 Vannes, France
E-mail address: `Frederic.Matheus@univ-ubs.fr`

François Maucourant, IRMAR, Université Rennes 1, 35042 Rennes Cedex, France
E-mail address: `francois.maucourant@univ-rennes1.fr`